U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

DOE/OE
National SCADA Test Bed
Fiscal Year 2008 Work Plan

APPROVED FOR EXTERNAL USE
(REVISED 07/28/2008)

NSTB

Enhancing control systems security in the energy sector

Fiscal Year

2 0 0 8

Work Plan

A plan of work for the National Laboratories that form the National SCADA Test Bed:

Argonne National Laboratory

Idaho National Laboratory

Oak Ridge National Laboratory

Pacific Northwest National Laboratory

Sandia National Laboratories

FOREWORD

The Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) created the National SCADA Test Bed (NSTB) program with the mission to reduce the risk of energy disruptions due to cyber attack on control systems. So far the program's projects have uncovered a multitude of knowledge that has already increased the security of our energy control systems around the country. Since its inception, the program has formed valuable links between the government, the energy sector, and national laboratories to conduct research and development in the area of cyber security. Through these partnerships, the DOE NSTB Program has identified ways to rapidly and effectively develop, integrate, and sustain security improvements.

The NSTB Team

Created in 2003, NSTB provided the energy sector (electric, oil, and natural gas) with an exclusive national resource for identifying and solving today's SCADA (Supervisory Control and Data Acquisition) and control system vulnerability issues, testing new and existing equipment, and developing secure architecture designs and technology advances. NSTB is a multi-laboratory partnership that draws on the integrated expertise and resources of the Argonne, Idaho, Oak Ridge, Pacific Northwest, and Sandia National Laboratories.

NSTB combines a unique range of specialized laboratory resources to create a realistic testing environment for SCADA communications and control systems. The national test bed enables systems to undergo a level of rigorous testing that would be impossible to perform on systems in active service. The test bed provides a safe and isolated, yet authentic environment for testing and evaluating control system vulnerabilities and mitigation strategies. The NSTB team's primary goals are to accomplish the following:

- Raise industry awareness of control system cyber security vulnerability issues and mitigation techniques.
- Collaborate with industry to identify, assess, and mitigate current SCADA system vulnerabilities.
- Work with industry to develop near-term solutions and risk mitigation strategies for existing control systems.
- Conduct R&D to develop next-generation architectures for intelligent, inherently secure, and dependable control systems and infrastructures.
- Support development of national standards and guidelines for more secure control systems.

Vendors accounting for more than 80% of new control systems entering U.S. energy markets have assessed or are assessing their systems at the test bed, and many have already used NSTB recommendations to design and distribute hardened systems and software patches to existing customers. NSTB has helped to raise industry awareness of system vulnerabilities, develop near-term cyber security solutions, and design next-generation architectures for intelligent, secure control systems.

Roadmap Implementation

In 2005, DOE/OE and the U.S. Department of Homeland Security (DHS) collaborated with the electric, oil, and natural gas sectors and with Natural Resources Canada to facilitate development of an industry-driven roadmap for securing energy sector control systems. The resulting *Roadmap to Secure Control Systems in the Energy Sector* outlines a strategic plan for protecting the electric, oil, and natural gas sectors from intentional cyber assault within ten years. The roadmap defines the vision, goals, milestones, and priority activities that will be pursued by industry and government to secure all energy control systems from intentional cyber attack.

The Roadmap provided a framework for integrating the diverse public and private efforts currently addressing vulnerabilities in our critical energy control systems across four industry-defined strategies: measure and assess security posture; develop and integrate protective measures; detect intrusion and implement response strategies; and sustain security improvements. It is now being used by energy companies, vendors, industry organizations, and federal agencies to guide and align investments in control systems security.

To enhance the Roadmap's effectiveness, DOE/OE NSTB Program created the interactive energy Roadmap (ieRoadmap), an online database where industry can map its R&D efforts for achieving Roadmap goals, evaluate its progress, and discover collaborative opportunities for future projects. The ieRoadmap to date features more than 80 energy sector control system security-projects submitted by more than a dozen public- and private-sector organizations.

Furthermore, in 2007, the DOE/OE NSTB program facilitated the formation of an Energy Sector Control Systems Working Group (ESCSWG) under the Critical Infrastructure Partnership Advisory Council (CIPAC). The efforts of the ESCSWG are designed to foster private and public collaboration to improve control systems security in the energy sector. The ESCSWG will have these key functions:

- Provide advice and guidance for Roadmap implementation
- Identify critical gaps and overlaps in research, training, practices, etc.
- Ensure roadmap milestones and priorities are accurate and relevant
- Help measure progress toward Roadmap goals and milestones
- Harmonize Roadmap with other industry initiatives; revise as required
- Help identify and map existing projects and activities using the online interactive energy Roadmap tool (ieRoadmap)
- Recommend and/or help launch specific projects or activities
- Increase awareness of control systems security issues within the energy sector
- Help establish the business case for investment in cyber security

The ESCSWG consists of senior representatives from the energy, and government sectors, as designated by the Electric and Oil & Natural Gas Sector Coordinating Councils and the Government Coordinating Council for Energy.

In a report to the U.S. president, the National Infrastructure Advisory Council (NIAC) recognized the Roadmap's success in developing and implementing cyber security solutions for control systems. The report recommended that all critical infrastructures adopt the Roadmap's goal of securing control systems against loss of critical function from intentional cyber attack by 2015. It also recommended that the Department of Homeland Security and other sector-specific agencies collaborate with their partners to create their own sector-specific roadmaps using the energy sector's Roadmap as a model. In March 2008 the Roadmap to Secure Control Systems in the Water Sector was developed by the Water Sector Coordinating Council (WSCC) Cyber Security Working Group (CSWG) with support from the Department of Homeland Security National Cyber Security Division and American Water Works Association[1].

Multi-Year Plan

Although many cyber security solutions will originate from the private sector, the transfer of these solutions involves national leadership, effective partnerships, and a shared vision of the future.

[1] http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf

Accordingly, the DOE/OE NSTB Program has closely aligned its efforts with the Roadmap, DOE/OE Mission, its unique capabilities and resources, ESCSWG recommendations, the National Strategy to Secure Cyberspace, HSPD-7, and additional federal efforts and policy guidance. The synthesis of this guidance was effectively realized through the establishment of a *DOE/OE NSTB Multi-Year Plan*.

The Plan defined an NSTB program goal to reduce the risk of energy disruptions due to cyber attack on control systems. To achieve this goal, the Plan established a coherent long-term strategy for improving the cyber security of control systems in the energy sector through program activities focused on developing next-generation control systems technology, conducting systems vulnerability assessments, developing end-to-end risk modeling and simulation capability, and partnering with public and private energy sector stakeholders to raise security awareness and leverage resources. These four program activity areas provide a sound foundation for collectively enhancing the security and reliability of the energy infrastructure. With the creation of the Plan, the DOE/OE NSTB Program and its partners have a clear path to a reliable, secure future.

NSTB Helping Industry Meet Roadmap Goals

To help support NSTB's efforts to enhance control system security in the energy sector, DOE/OE recently awarded nearly $8 million to fund five industry-led, cost-shared projects:

- Cyber Audit and Attack Detection Toolkit. Will extend the capability of existing vulnerability scanning tools to evaluate SCADA security configurations, and develop templates for a security event monitoring system. (Lead: Digital Bond; Partners: Tenable Network Security, OSIsoft, Constellation Energy, PacifiCorp, TVA)
- Detection and Analysis of Threats to the Energy Sector (DATES). Will develop intrusion detection systems (network-, host-, and device-level), event correlation framework, and a sector-wide, distributed, privacy-preserving repository of security events. (Lead: SRI International; Partners: ArcSight, Sandia National Laboratories, ERCOT)
- Hallmark Project. Will commercialize the Secure SCADA Communications Protocol (SSCP), which marks SCADA messages with a unique identifier that must be authenticated before the function is carried out, ensuring message integrity. (Lead: Schweitzer Engineering Laboratories; Partners: Pacific Northwest National Laboratories, CenterPoint Energy)
- Lemnos Interoperable Security Program. Will conduct testing, validation, and outreach to increase the availability of cost-effective, interoperable security solutions for Internet Protocol (IP)-based communications. (Lead: EnerNex Corp.; Partners: Schweitzer Engineering Laboratories, TVA, Sandia National Laboratories)
- Protecting Intelligent Distributed Power Grids Against Cyber Attacks. Will develop a risk-based critical asset identification system and optimize integrated and distributed security systems to establish the best topology for networking security components. (Lead: Siemens Corporate Research; Partners: Idaho National Laboratory, Rutgers Center for Advanced Energy Systems)

The NSTB Program and its national laboratories are working closely with all industry project leads to harmonize their control system security initiatives with NSTB and Roadmap goals and minimize duplication of efforts. For several projects, NSTB's national laboratory subject-matter expertise, unique capabilities, and specialized facilities are being leveraged in the R&D process. DOE's National Energy Technology Laboratory, through the NSTB Program, will manage these projects, which are expected to be completed over the next two to three years. Although not contained within this Plan, complete fact sheets on each industry-led project are available on the NSTB Program website at www.oe.energy.gov/controlsecurity.htm.

Work Plan

The DOE/OE NSTB Program was created with a clear understanding that improving the security of SCADA and control systems is integral to protecting the energy infrastructure and the sectors it serves. As defined in its Multi-Year Plan, all FY2008 DOE/OE NSTB program activities are aligned under four project areas:

- **Next-Generation Control Systems.** Research and development concentrates on accelerating the development and deployment of hardened control systems with built-in security.
- **System Vulnerability Assessments.** Rigorous tests reveal exploitable systems vulnerabilities and encourage development of system fixes.
- **Integrated Risk Analysis.** Developing means for stakeholders to assess their security posture will hasten the ability to mitigate potential risks.
- **Partnership & Outreach.** Active partnerships engage all stakeholders and encourage collaborative developments and dissemination of critical security information.

DOE/OE NSTB has a generous number of ongoing activities in each area, all of which are detailed in the following pages.

Project Alignment with NSTB Program Elements

Project	Next Generation Control Systems	Integrated Risk Analysis	System Vulnerability Assessments	Partnership & Outreach
Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM)	✓			
AMI-SEC Acceleration Project (A.S.A.P.)	✓			
Anomaly Detection and Distributed Active Response for Control Systems	✓			
Applicability and Security of Wireless Communication in the Electric Sector	✓			
Cyber Detection & Protective Technology Development	✓			
Inter-Control Center Communications Protocol (ICCP) Security Assessment	✓			
Protocol Analyzer	✓			
Secure Data Transfer	✓			
Security State Monitor Visualization Tool	✓			
Trustworthy Communication Architecture for Converged SCADA Applications	✓			
Trustworthy Cyber Infrastructure for the Power Grid (TCIP)	✓			
Wireless Sensor Networks and Applications to Electric Power Systems	✓			
Annual Risk Analysis Workshop		✓		
Consequence Modeling		✓		
Impact Analysis of Cyber Attacks on Control Systems		✓		
Plausible Threat Characterization		✓		
Virtual Control System Environment (VCSE)		✓		
Assess Control Systems in Test Bed Facilities			✓	
Cyber Vulnerabilities in Industry Technologies			✓	
Identification of Cyber Vulnerabilities in Electrical Substations			✓	
On-Site Vulnerability Assessment			✓	
Industry Conference Participation				✓
NERC CSSWG Support				✓
SCADA Security Workshops				✓

Table of Contents

NEXT GENERATION CONTROL SYSTEMS

Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM)

Lead: Sandia National Laboratories, Bryan Richardson

Purpose

The Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM) work package will provide energy sector utility owners a software toolkit for mapping and visualizing their control system networks to help assess their network security posture. The source code and documentation for the ANTFARM tool will be made available to interested parties via open source, under a "no-fee," general-purpose license agreement. Future code development and enhancements made to the ANTFARM tool will be shared by the community at large, thus providing a cost-effective way for developing much needed network assessment tools for control system environments.

Background

Conducting active, online scanning and reconnaissance activities on a control system network to help facilitate the remote mapping of the network can be detrimental to the control system due to the fact that some (if not most) control system software responds unpredictably to unexpected messages and queries. Thus, there is a need for tools capable of conducting remote mapping of networks using only passive techniques.

The ANTFARM software tool is the result of many conversations about how to improve and simplify network assessments and the tools needed to better understand networked systems and their topology. The core idea behind ANTFARM is to be able to easily utilize multiple sources of information that describe a system and correlate the data in a database. These sources of information include, but are not limited to, existing tools such as SNMP[2], Traceroute[3] (or Tracepath), network traffic sniffers (such as Wireshark[4] or tcpdump), and port/vulnerability scanners (such as nmap[5] and Nessus), and existing data such as network equipment configuration files, firewall configuration files, and traffic logs. Once correlated, the resulting data can be used to depict a visual representation of the network being mapped.

Scope and Technical Approach

A solid core of source code and detailed documentation focusing on the accurate insertion and correlation of data into the ANTFARM database will be developed. DOE owns the rights in copyrightable works (e.g. ANTFARM software) created at Sandia. Therefore, Sandia National Laboratories (SNL) must request permission from DOE/OE to distribute.

Once the necessary open source requests to SNL and DOE/OE have been accepted, this core source code and documentation (including our vision for future enhancements) will be made available to the general public for further development and usage via an open source repository website such as *SourceForge*, *RubyForge*, and/or *Google Code*.

By open sourcing the ANTFARM software tool, we make the tool's source code available to an infinite number of talented and capable programmers, which generally leads to the secure, concise, and rapid development of software projects. Along these same lines, open sourcing ANTFARM will also make the

[2] http://en.wikipedia.org/wiki/simple_network_management_protocol
[3] http://en.wikipedia.org/wiki/traceroute
[4] http://en.wikipedia.org/wiki/wireshark, http://en.wikipedia.org/wiki/tcpdump
[5] http://en.wikipedia.org/wiki/nmap, http://en.wikipedia.org/wiki/nessus_(software)

tool easily available to users needing a way to passively map networks, such as control system network security personnel.

Subtask 1: Document ANTFARM software toolkit and Sandia's vision for future enhancements
Develop a document describing the path for future development of the ANTFARM tool. This document will describe the input /output requirements of the tool, features and limitations of the tools, a preliminary operator's manual, and describe a wish-list of follow-on features/capabilities for the tool.

Subtask 2: Enhance and document ANTFARM source code
Restructure the existing ANTFARM source code to utilize Ruby's ActiveRecord[6] package for accurate and secure insertion of data into the ANTFARM database. Existing data parsing scripts will be refined to utilize ActiveRecord as well. While restructuring and refining the existing code, the code will be documented to ease future developments of the tool.

Subtask 3: Publish ANTFARM software (open source)
Complete the necessary paperwork to allow SNL and the DOE/OE to open source the ANTFARM software. Once these requests have been accepted, the ANTFARM software, along with its supporting documentation, will be hosted on a publicly accessible website (such as *RubyForge*) as a software network tool.

AMI-SEC Acceleration Project (A.S.A.P.)

Lead: Idaho National Laboratory, Dave Kuipers

Participants: EnerNex, Intelguardians, Electric Power Research Institute (EPRI), 12-14 Utilities/Independent System Operators (ISOs), others TBD

Background

The technology concept of Advanced Metering Infrastructure (AMI) involves extension of advanced communications beyond the substation to home and commercial end users. The creation of this ubiquitous communication system reaching the remote ends of the grid places us in completely new and unexplored territory. We will have millions of end points, direct control of load and limited physical access control options on assets within easy reach of cyber threat actors. This project will analyze emerging AMI technologies and architectures for cyber vulnerabilities, including selections from the following:

Topologies: Aggregation, Backhaul, Mesh Ad-hoc / Sited, Hierarchical Ad-hoc / Sited, Custom, Other
Technologies: WiMax, CDMA (Cellular), GPRS, GSM (Cellular), EVDO, Z-wave, Custom, Other
Frequencies: ISM bands 900 MHz, ISM bands 2.5 GHz,
Coding Schemes: OFDMA, DSSS, FHSS, MIMO, Custom, Others
Stations/Endpoints: Head-ends, Relays, Collectors, Take-out points, Pole-tops, Aggregate points, Meters, Repeaters, Custom, Others

The project will support the industry work group in identifying potential security solutions and recommended practices for the deployment of AMI infrastructures through a detailed analysis report.

[6] Active record is a software design pattern for accessing data in a database. See a formal definition at http://en.wikipedia.org/wiki/active_record_pattern. An active record framework exists specifically for the Ruby programming language, and can be found at http://ar.rubyonrails.com.

Scope and Technical Approach

Provide cyber security vulnerability analysis of technologies, devices and communications related to AMI. The scope of this task includes infrastructures used in the Neighborhood Area Network (NAN), the Home Area Network (HAN) to include the meters, and the AMI WAN, inclusive of the aggregate points and head ends as applicable. The targeted technologies will be those currently deployed and being procured for deployment from the industry leaders. We have to target the highest market shares to achieve the broadest benefit. Selection of technologies will be a collaborative effort between all project partners, including utilities, EnerNex, Idaho National Laboratory (INL), and others.

The security and interception analysis of the technologies deployed in these infrastructures is a new and critical process due to the sensitivity of the data and control being communicated. The breadth of the technologies available for use in these configurations is enormous. The analysis will have to be limited to the selected configurations determined by the industry market share leader.

Anomaly Detection and Distributed Active Response for Control Systems

Lead: Oak Ridge National Laboratory, Wayne Manges

Purpose

Cyberspace Sciences and Information Intelligence Research (CSIIR) of Oak Ridge National Laboratory (ORNL) will develop the Silent Storm technology for distributed cyber-defensive active response to cyber attacks against Process Control and SCADA systems. This statement of work directly addresses the research and development of the Silent Storm technology and the demonstration of Silent Storm's ability to detect and thwart the problem of cyber intrusion on SCADA systems.

Developing this technology, we will apply the following innovative advances:

- Ubiquitous Network Transient Autonomous Mission Entity (UNTAME) research platform will collect network traffic at the protocol level and perform anomaly detection analysis. UNTAME is a cutting-edge prototype development of a software framework for distributed network sensing and system analysis. This distributed computational intelligent framework addresses the issues of real-time situational awareness, and distributed cyber-defensive active response to cyber attacks.
- The Heuristic Identification and Tracking of Insider Threat (HIT-IT) system is a distributed, hierarchical, multi-level, hybrid intrusion detection system. The system uses client-server architecture and provides scalability because of its hierarchical nature. HIT-IT audits at the application, transport, and network layers of the Internet protocol stack, and monitor the user, kernel, and system resource levels. It combines a traditional rule-based approach with data mining to create a hybrid system. HIT-IT has four main components: the sensor, the threat management server (data-mining element), a database, and the command and control utility.
- The THYME framework will be used to emulate a continuous system and a PLC. Modified NS2 will be used to emulate different network protocol stacks. A control scenario involving four nodes will be developed. The scenario will involve a continuous physical system controlled over a discrete packet-based network. The control signal will be sent over a SCADA network. DNP3 and MODBUS will be emulated. The packet capture is used to replay the scenario in the presence of a distributed intrusion detection system. An intrusion scenario will be developed to exploit the vulnerabilities of DNP3 and MODBUS.

Background

The Silent Storm technology seeks to demonstrate distributed cyber-defensive active response to cyber attacks on process control systems (PCS) and SCADA systems. CSIIR/ORNL will leverage key research performed by the principal investigator and research staff to deliver a prototype demonstration of the technology. This technology represents efforts to sustain research in addressing immediate challenges in energy security.

Scope and Technical Approach

The research and development necessary to demonstrate the Silent Storm technology will be undertaken during this Year (spanning FY08 and FY09). By the end of Project Year, ORNL will laboratory deploy a vertically integrated stand-alone demonstration prototype that highlights the proposed technology. This prototype will serve as a gate to allow the Government sponsor to evaluate our technical skills and our product's potential utility.

1. Develop System Architecture Document: We will develop a system architecture document and System API as a component of product documentation and to drive the software development process in a cohesive way.
2. Develop Distributed Intrusion Detection Sensors: We will develop a distributed intrusion detection sensor suite for use with the UNTAME computational intelligence framework.
3. Develop Intrusion Detection Rule Set: We will develop an initial collection of intrusion detection rules for use in the distributed rule engine of UNTAME.
4. Develop and Simulate traffic analysis of PCS: We will develop a collection of rules for data fusion from the simulated traffic analysis of the PCS.
5. Develop and Integrate the UNTAME Subsystem: UNTAME will be adapted to the distributed intrusion detection system. This will allow the system to gracefully degrade if it is included as part of a network attack.
6. Deploy Test Network: We will deploy a test system to the CSIIR Group sub-domain for the initial demonstration of Silent Storm.
7. Evaluate and Test: ORNL will perform spiral development testing of the software suites at 3 and 6 months.
8. Demonstration: ORNL will configure system and perform a technology demonstration.

Applicability and Security of Wireless Communication in the Electric Sector

Lead: Pacific Northwest National Laboratory, Mark Hadley
Participants: Oak Ridge National Laboratory, others TBD

Purpose

The use of wireless technologies is an important topic of current interest to electric power utilities. Applications of wireless technologies are being made for communication within a substation, between substations, between the control center and substations, and also to improve situational awareness of transmission and distribution lines. Appropriate use of wireless technologies, security of wireless technologies, and the impacts of wireless upon regulatory requirements all must be addressed. This effort will focus on energy sector application of wireless technologies.

Background

Wireless technology has been used in the electric sector for decades. Acceptable and trusted wireless communication technologies include analog microwave and SCADA radio. In addition, the corporate network may support distinct wireless networks for staff and visitors. The use of cell phones and pagers by engineers is not only acceptable but required. Today vendors are including other wireless technologies such as Zigbee, Bluetooth and WiFi in their product offerings. The utility is faced with the need to address the appropriate use and security of these new technologies in new application environments.

Industry has expressed concern over the use of wireless and its impact upon their ability to comply with regulatory requirements. The North American Electricity Corporation's Critical Infrastructure Protection 005 (NERC CIP-005) standard requires a utility to monitor and control their electronic security perimeter. This task is challenging with a wired network but compliance becomes much more difficult in a wireless setting. Wireless technologies are appearing in substations, in automated meter-reading infrastructures, and in new control center to substation communication environments. Utilities are at a cross road where wireless must be embraced; it can no longer be ignored. This project will review various technologies to identify appropriate policies and procedures, develop industry and technology-specific security practices, and create training and vulnerability demonstration materials for industry.

Goals and Benefits

The *Roadmap to Secure Control Systems in the Energy Sector* identifies the use of wireless communication as an emerging trend affecting future control system security. A prime factor concerning the future use of wireless is the acceptance of wireless technology by future energy engineers. A recent UtiliPoint article stated that upwards of 60% of current utility engineers will retire in 5 to 10 years. These engineers will be replaced by a younger generation that readily accepts and expects to use wireless on the job. Industry must embrace the potential use for wireless in order to adequately secure the intentional and unintentional use of wireless technologies.

Industry will benefit by a review of each technology that includes a discussion on unique characteristics, identifying the specific wireless technology can be used, where the specific wireless technology should not be used, and methods to secure the wireless technology. A large aspect of this effort involves training and demonstrations for energy sector personnel. Compromising wireless networks can take a matter of minutes.

The primary goals of this effort are to increase awareness regarding wireless use, provide white hat training and demonstrations to improve understanding of wireless security vulnerabilities, and provide industry with applicable use scenarios and information.

Scope and Technical Approach

This project will review various technologies to identify appropriate policies and procedures, develop industry and technology-specific security practices, and create training and vulnerability demonstration materials for industry. This project will utilize a phased approach to examine current and emerging wireless technologies to identify appropriate use. Two reports are envisioned for each technology. The first will address appropriate use and the second security. Appropriate use topics will identify where a specific technology can be used, where the technology should not be used, what products are available that support the technology, how to select an appropriate technology, and what are the communication characteristics of the technology. A security paper that identifies publicly available vulnerabilities and mitigations strategies will be developed. Industry momentum is currently focused on WiFi, WiMax, Bluetooth, and Zigbee technologies.

A second focus area is white hat / white box testing of wireless technologies. This effort includes conference participation and presentation activities to increase wireless security awareness. This effort will be led by the technical staff at Pacific Northwest National Laboratory (PNNL) involved in the operation of multiple wireless networks (mesh, point-to-point, personal area, etc.) and will address security issues such as boundary protection, rogue device detection, and defense-in-depth implementations. Security myths (e.g. a licensed frequency protects my network, we use a Yagi antenna so a signal cannot be injected) regarding wireless networking must be addressed as part of this effort.

A third technical area addressed is training for utility staff to improve understanding of wireless technologies, identification and control of wireless technologies, technology selection, and regulatory compliance.

Cyber Detection & Protective Technology Development

Lead: Idaho National Laboratory, Dave Kuipers
Participants: TBD

Background

The task is to develop and implement detection and protection capabilities within the vulnerability assessment, intrusion detection/prevention and network forensics product arena. Control systems are particularly vulnerable to cyber exploitation as new vulnerabilities are announced as the system owner must wait for the control system vendor to release a patch or update to resolve the vulnerability. Even after a patch is released, it may be some time before an owner can appropriately test and apply the patch. During this “window of exposure,” system owners are still vulnerable and have little if any means to detect intrusion or protect their systems. Legacy control systems are often more vulnerable due to reduced or non-existent vendor support for vulnerability patching.

Detection and mitigations technologies are essential for isolation and protection of the sensitive data interface and integration into SmartGrid systems. This research is critical to provide optimization of data communications protection in support of this expanding communications integration of the nations electrical grid systems. This effort addresses several Roadmap priorities including: adapting intrusion prevention for application to control systems, developing intrusion detection and protection products for control systems, develop sensors with mechanisms to detect and report anomalous activity and develop cost effective gateway security by improving the capability of existing gateway technologies for control systems.

Scope and Technical Approach

The results from earlier assessments of the control system provide a substantial benefit from the standpoint that some vulnerabilities are already known and in several cases the exploits are already developed. This greatly reduces the effort required to get to the point in the process where the exploit is being actively used to disrupt system operation. The SCADA systems of interest are currently installed in the SCADA Test Bed with ready connectivity into representative operational environment that will support typical control system data traffic.

This effort will require participation by third party information security vendors, control systems vendors, and potentially utility asset owners. Control systems currently available in the SCADA Test Bed will be

used to support this task and the system vendor will be requested to provide limited technical support establishing an operational system. Using the results obtained in prior assessments, exploits will be developed and launched against identified control system vulnerabilities, and potentially against additional vulnerabilities identified during this process.

As the exploits are performed, network traffic protocol analysis as well as host operating system analysis will be performed to understand the behavior induced by the exploit. These behaviors can then be translated into the appropriate algorithms for open source intrusion detection, intrusion prevention, vulnerability assessment and network forensics technologies. Using open source technologies provides an avenue for all results obtained during the project to be presented to control system and third party security vendors in a neutral format. This allows the vendors to potentially incorporate the results into their own technologies, or provide the information to their customers; thereby improving the overall ability of the security vendors, and the owner operators to secure their environment.

Inter-Control Center Communications Protocol (ICCP) Security Assessment

Lead: Idaho National Laboratory, Dave Kuipers
Participants: LiveData, SISCO, ABB, AREVA, Siemens

Background

The Inter-Control Center Communications Protocol (ICCP) is used extensively in the electric utility industry for communicating status data, commands and general text information between electric grid control centers. The information transmitted over ICCP is critical to the efficient operation of the grid and corruption of the data could have a significant financial impact on grid operations. Data communications integration into SmartGrid concepts will require secure open protocol communications for connectivity of multiple disparate data sites; such as distribution, generation, and transmission system electrical substations, control centers, and management centers. Since ICCP is in use by most of the industry for communications across geographical regions and connection of businesses and applications it will be a factor in the SmartGrid integrated communications methods. Additionally, since most of the data passed between control centers originates in the SCADA/PCS, the ICCP communications link could have vulnerabilities, that when exploited could allow access from one control center to the control system of another entity.

An assessment was performed in FY2007 whose main objective was to identify vulnerabilities in the protocol stacks of the two primary ICCP stack providers, SISCO and LiveData. This assessment uncovered several vulnerabilities that were communicated to the applicable vendor; both vendors have been extremely proactive in mitigating the problems found in their respective products.

Additional funding is required to complete this effort in FY 2008. ICCP is a very complex protocol, one of the few to implement all seven layers of the OSI stack and some layers have multiple sub-layers. The FY 2007 assessment was able to address portions of all of these layers, but additional work is required to finish the vulnerability assessment and test mitigations that the vendors are implementing.

Additionally, the products of the SCADA vendors need to be tested. The FY07 assessment demonstrated that some of the vulnerabilities in the protocol stacks may be more severe depending on which operating system is used. The products that were tested ran on a Microsoft Windows platform. Some of the vendors use UNIX or LINUX platforms for their products, which in at least one case could have made a

vulnerability exploitable. In addition, each vendor's application program interface (API) was not able to be tested, which could be the source of additional vulnerabilities.

Scope and Technical Approach

A test plan will be updated to address vulnerabilities, potential exploits, installation/ configuration guidelines, functionality impacts, and mitigation strategies applicable to ICCP.

This task will include expanding the scope of the ICCP software tool developed during the previous phase. This will allow the stacks of both vendors to be fully tested. A further task will apply the tool developed and further expand its scope to allow the products of each of the major SCADA vendor's products to be tested. This work will be performed under existing cooperative research and development agreements (CRADAs) with SISCO and LiveData and with each of the primary SCADA vendors. With the existing status of CRADAs, assessments, and support, the primary SCADA vendors will include ABB, AREVA, and Siemens. If vulnerabilities are discovered, an attempt will be made to exploit them to gain root access on the targeted system(s). Any vulnerabilities identified and respective recommended mitigations will be provided to the software vendors. Patches to the vulnerabilities will be released by the ICCP vendors to their customers which will decrease the possibility of cyber access to a SCADA/PCS network via ICCP communication.

Protocol Analyzer

Lead: Pacific Northwest National Laboratory, Mark Hadley

Participants: Applied Systems Engineering, Frontline, Siemens, Telvent, Schweitzer Engineering Laboratories, Triangle MicroWorks, CenterPoint Energy, others TBD

Purpose

The purpose of this project is to provide operational support to electric utilities deploying the Secure SCADA Communications Protocol (SSCP) to Protocol Analyzer and Test Set vendors. Utilities employ Protocol Analyzers to troubleshoot communication problems and monitor communication. Control system vendors use Test Sets to simulate master or field devices to test support for new protocols. Current Protocol Analyzer and Test Set product offerings do not support the SSCP. This project will add support for the SSCP to both commercial and open source Protocol Analyzers and commercial Test Set tools.

Background

PNNL has developed a method to authenticate serial SCADA communications to meet the telemetry and control requirements in the electric sector. The SSCP project team utilized a board of industry advisors to guide research and development activities. The advisory board was staffed by asset owners, industry consultants, cyber security experts, and grid operators. The advisory board recommended that the solution:

- Provide message authentication without encryption
- Be embedded onto SCADA master servers
- Support modern and legacy devices
- Introduce minimal latency into the communication stream
- Provide unique keys for each remote device
- Collect security events

- Concentrate on serial communication

The SSCP is currently being transferred to control system industry vendors. The Hallmark Project is a joint effort between PNNL, Schweitzer Engineering Laboratories (SEL), and CenterPoint Energy to create a bump-in-the–wire product for legacy systems. Siemens is currently embedding the SSCP into their remote terminal unit (RTU) and communication server products in support of current and future deployment. Telvent is the most recent vendor to express interest in incorporating the SSCP into their product line.

The SSCP is making market penetration and will be available for utilities in the near future. In order to support the operational need to monitor communication, protocol analyzers must be able to interpret the SSCP header and authenticator. Vendors such as SEL, Siemens, and Telvent can use the Test Set to evaluate and expedite their SSCP development efforts.

Goals and Benefits

The *Roadmap to Secure Control Systems in the Energy Sector* identifies "Widespread implementation of methods for secure communication between remote access devices and control centers" as a key milestone. Development and commercialization of the SSCP is currently achieving that milestone. Most security vendors approach this milestone by creating encryption solutions. However, with encryption solutions, the ability of the utility to monitor communication is limited or diminished. The cipher text produced by the encryption algorithms cannot be interpreted by protocol analyzers, resulting in a loss of operational capability and perhaps reliability. The SSCP does not alter the original control system message; the message is encapsulated by a header and an authenticator. The benefit is that people and/or protocol analyzers that understand the SSCP can interpret both the SSCP and the original message.

The ability to monitor communication is critical to daily operations. Serial control system communication can be problematic due to noise, media, or misconfiguration of communications equipment. Asset owners have made substantial investments in cable systems to support both redundancy and the ability to monitor communication. Adding the SSCP to control system protocol analyzer vendor products will allow asset owners to utilize their infrastructure investments and also perform troubleshooting functions.

The ability of new vendor deployments of the SSCP will be hastened by creating a test set to simulate master (operations center side) or remote (substation side) communication. While the SSCP only provides authentication, it involves a complex set of algorithms and settings. The Test Set tool will enable vendors to ensure interoperability with other vendors, correct implementation of cryptographic algorithms, support for all necessary packet types and configuration options. Both commercial products and open source solutions will be targeted during this effort. A final benefit will be quicker adoption by EMS vendors at lower cost.

Scope and Technical Approach

The SSCP is a well defined technology being incorporated into vendor products. During the initial technology transfer engagements, PNNL staff learned that we must establish relationships, make ourselves available to answer questions, provide both technical support and implementation guidance, and package the technology in a manner that supports the vendor's requirements. One cannot simply push the technology "over the fence" to the vendor and walk away. PNNL will build upon these lessons learned when engaging new vendors.

To identify which protocol analyzer and test set vendors to approach, PNNL will conduct a short survey of utilities. The SSCP protocol specification, implementation guidance, and source code will be provided to these commercial Protocol Analyzer vendors (e.g. Applied Systems Engineering, Frontline) to expedite incorporation of the SSCP into their products. PNNL will establish strategic relationships with these

vendors, test their implementations to ensure compatibility and proper implementation, and participate in joint marketing efforts (e.g. flyers, press release, conference presentations).

In addition to commercial vendors, open source solutions will be targeted during the project. Most open source solutions today target routable protocols and network interfaces. In order to incorporate the SSCP, support for serial interfaces and both block and streaming serial traffic must be included. After serial traffic can be processed, the SSCP will be incorporated into the open source solution (e.g. Wire Shark).

Secure Data Transfer

Lead: Pacific Northwest National Laboratory, Bryan McMillan
Participants: Argonne National Laboratory, others TBD

Purpose

The purpose of this project is to provide a defense-in-depth methodology and technical solution to support the transfer of data from a control center network to critical business systems in a manner that is secure, timely, simple to operate, and supportive of regulatory requirements.

Background

The transfer of data from a control center network to the corporate network is an ongoing problem to be addressed. Data is transferred for a variety of reasons including customer billing and planning applications. Data must be transferred in a timely and secure manner, and it is common for recommendations to simply require that a demilitarized zone (DMZ) be used. However, the components that comprise the DMZ, DMZ functions, and the security levels provided by the DMZ are often absent. This project will identify requirements for secure and timely data transfer, develop a control system specific solution, and create a best practices guide for asset owners to implement the technology.

The data transfer process between the corporate and control center networks is complicated because the networks have different security postures. The control system network is more secure than the corporate network. In addition, regulatory requirements specify the ability to control the electronic security perimeter of the control center network (e.g. NERC CIP-005 R2). A properly configured DMZ can provide compliance with this requirement. However, a poorly defined DMZ will cause a utility to be out of compliance and subject to findings and fines.

Goals and Benefits

Data provides both knowledge and power. According to a Wall Street Journal article, we have moved from management by objectives and total quality management to management by data. We are becoming a data-driven society, and decision makers in all industries, including utilities, will require more access to data. This project addresses the need to securely obtain data, the Roadmap goal to “Develop and Integrate Protective Measures” and the specific milestone “Secure connectivity between business systems and control systems within corporate network.” Data obtained and stored in an insecure fashion leads to vulnerabilities that can be exploited by an adversary.

Utilities typically utilize a minimal defense layers to secure data transfer. For example, one common implementation utilizes a file share or database with varying access permissions; the control center is given write access and the corporate network read access. Other implementations utilize public key infrastructure and digital signatures to validate communication. Still others utilize air gap technologies.

The goals of this project are to identify requirements, design a solution based upon identified requirements, and develop a solution that meets the requirements. Benefits of this approach include:

- A repeatable DMZ implementation for industry
- Multiple layers of defense in a simple solution
- The ability to support both Windows and UNIX environments
- Timely data transfer
- A well-defined electronic security perimeter
- Regulatory compliance
- Removal of implicit trust

Scope and Technical Approach

This project will utilize key personnel at both PNNL and Argonne National Laboratory (ANL) to provide both electric and gas industry knowledge. A group of industry advisors will be used to provide examples of solutions currently in use, identify shortcomings with those implementations, and also identify requirements for the ideal solution. The first project task will be to assemble the industry advisory board of industry.

This project will utilize the Electric Infrastructure Operations Center (EIOC) at PNNL as a research and development environment. The EIOC is a logically and physically isolated network at PNNL that simulates the control center and corporate network environments. The EIOC has a higher security posture then the main PNNL corporate network and can be connected to the PNNL network via a DMZ. The EIOC also contains a complete AREVA EMS, SCADA communication from a local utility, and wide area measurement system data feeds. Together these data types and systems provide ample data for use by simulated systems residing on the PNNL corporate network.

The project will utilize the advisory board to gather requirements, review the requirements document, and review the high level design. PNNL staff from the classified networking world will provide guidance on solutions from those environments that perform similar functions. A detailed design will be created and reviewed, and development of a technical solution will begin. During year two, a third advisory board meeting will be held to review the initial proof of concept implementation and identify one or more field test locations. The field tests will be used to measure latency and gather input for implementation guidance. In year three, the focus will be technology transfer to industry.

Security State Monitor Visualization Tool

Lead: Pacific Northwest National Laboratory, Mark Hadley

Participants: Siemens, Schweitzer Engineering Laboratories, CenterPoint Energy, SRI, EnerNex, Applied Systems Engineering, others TBD

Purpose

Cyber security has become a critical building block of safe and reliable grid operations. Deploying security technologies without monitoring their health and effectiveness provides electric companies a false sense of security. Companies must thoroughly understand their current security posture to determine system vulnerabilities and the actions required to address them. This project will help ensure that energy

asset owners have the ability to perform fully automated security state monitoring in real time of their control system networks and security technologies by creating an interactive visualization environment built to the demands and expectations of the energy sector.

Background

The control systems supporting our nation's energy systems were created with the objectives of high availability and safety as the highest concern. Cyber security was an after thought at best, resulting in an environment with a multitude of vulnerabilities. As security awareness increased, vendors began offering security products or security features in their control system products. Consider intrusion detection systems that offer signatures for control system protocols, cryptographic protection devices for both network and serial communication, and protocol offerings that utilize digital signatures to provide authenticity.

Likewise, situational awareness of the power grid has also evolved over time. SCADA communication, with data samples occurring every two to four seconds, has been enhanced with phasor measurements samples occurring 30 times per second. The result is a better view of the health or status of the electric grid due to more and better information.

The reliability and availability of the power grid is also directly related to the confidentiality, integrity, and availability of cyber security technologies that are deployed to manage risk and to detect and mitigate attacks and vulnerabilities. This project will bring together elements from these deployed technologies into a visual environment to present the state of control system security measures and countermeasures thus providing asset owners with real time situational awareness of their security posture.

This real-time state monitor tool will provide the asset owner with a local view that can be also be aggregated to provide regional and national views. The security state monitor will provide many functions including:

- Event correlation across the control system, region, or nation
- Identify security concerns at a glance
- Provide the ability to interact with displayed information for detailed information
- Incorporate multiple data feeds and data formats (RSS, text, syslog, proprietary)
- Provide multiple output data feeds (less specific data for regional or national monitoring)

Goals and Benefits

The *Roadmap to Secure Control Systems in the Energy Sector* identifies a "Measure and Assess Security Posture milestone" of "a real-time security state monitor for new and legacy systems" to be commercially available. This project directly addresses this milestone.

A security state monitor that functions in real time is a requirement for and user of other Roadmap goals as well. The security state monitor must accept security status information from deployed protective measures and provide input to detect intrusion and implement response strategies.

In addition, the security state monitor can be implemented at the local, regional, or national levels to provide appropriate situational awareness of the cyber security posture. Tying the security state monitor to the national threat level provides the ability to visually see how the security posture changes with the threat level. For example, allowing remote access via a virtual private network (VPN) from the corporate network to the control center may be allowed when the threat level is green but will trigger an event that must be addressed when the threat level changes to orange.

The ability of current cyber solutions to capture and process cyber security events varies widely. Some technologies store logs locally, some do not store logs at all, and others integrate with logging services such as Syslog. One desired outcome of this project is the definition of a standard control system event reporting methodology that will make the event collection, correlation, aggregation, and reporting functions more efficient and consistent. The benefits of the technology include the ability to visually display the security posture of the utility's deployed cyber security solutions, the ability to trigger automated responses in the future in response to security events, and the ability to correlate events at the local, regional, or national level.

Scope and Technical Approach

In previous projects, an industry advisory board was successfully used to guide research and development activities. The advisory board also provided a mechanism to market the project to industry. This project will also utilize an advisory board of utility and energy industry organizations to guide visualization requirements, user interaction requirements, integration of threat levels, and lastly the correlation and reporting of events. This project will also coordinate logging functions with other DOE/OE funded projects (e.g. Hallmark, Lemnos) as well as commercially available technologies. A list of technologies from which security status data must be captured and items to monitor include:

- Perimeter Security
- Network Traffic Analysis
- Signature-based and anomaly-based intrusion detection systems (IDS)
- Secure Communication Solutions
- AMI Technologies
- Remote Access
- Wireless Technologies
- Physical Security
- Access Controls
- Threat Level

After the industry advisory board is assembled, the PNNL project team will prepare preliminary information in advance of the advisory board meeting. The information presented to the advisors includes project scope, representative display technologies, and information on event correlation and aggregation. The meeting will be held at PNNL's EIOC. This facility, designed as both a control center and research and development center, provides live data feeds from industry, visualization capabilities, and connections to multiple networks. During the first meeting, PNNL staff will capture information regarding which events should be monitored, how events should be related, and how events should best be displayed and/or reported.

After the first meeting, PNNL project staff will write the requirements document and design sample event reporting screens for review at the second advisory board meeting. During the second meeting, the documents and screen images will be reviewed in preparation for year two activities that include high level and detailed system design, data feed normalization, and prototype development.

Trustworthy Communication Architecture for Converged SCADA Applications

Lead: Pacific Northwest National Laboratory, Jeff Dagle
Participants: University of Illinois at Urbana-Champaign

Purpose

The objective of this project is to create a converged secure, real-time, monitored, and robust communications infrastructure for SCADA systems. This communication infrastructure is aimed at supporting a set of converged applications including but not limited to protection, monitoring and maintenance. This research program will provide a novel communications infrastructure, implemented as a middleware and toolkit, for energy control that is 1) **secure** with end-to-end encryption and authentication, 2) **real-time** with a Quality-of-Service managed network that provides strong guarantees, 3) **monitored**, with an intrusion detection system that provides alert correlation and 4) **integrated** to support a set of converged applications including protection, monitoring and maintenance.

Background

Many of the current energy infrastructure control systems are operating on technology designed before modern computing and communication systems emerged. This project has the potential to provide technology that will directly contribute to the vision and mission of the DOE/OE, paraphrased here as "Provide the best and most secure energy services available in the world, enhance the security and reliability of the energy infrastructure, and facilitate recovery from disruptions to the energy supply." Achieving that mission will be done through the development of an energy control infrastructure that is:

1. Secure with end-to-end encryption and authentication,
2. Real-time with a Quality-of-Service managed network that provides strong guarantees
3. Monitored with an intrusion detection system that provides alert correlation
4. Integrated for application convergence that delivers a multitude for services

The *Roadmap to Secure Control Systems in the Energy Sector* makes it clear that much has to be done to provide a secure environment for energy control. Near-term actions to develop and integrate protective measures are limited to distributing consistent training materials on cyber and physical security for control systems. Long-term actions include development of a next-generation control system that can survive malicious attacks without loss of critical functions. The security architecture proposed in this work is intended for such next generation control systems where commercial, off-the-shelf (COTS) devices, operating systems and software will be widely deployed and used. Furthermore, the proposed work on monitored, timely and secure communications will provide a complete systems context for the emerging security components.

This project will take a fundamental approach of designing solutions for secure, real-time and monitored communication systems that support power grid needs. This is a unique endeavor that leverages other related work but focus on a significantly more thorough design space exploration. It is likely that solutions approaches developed by this project will be implemented in other activities, such as GridStat, or lead to new capabilities that will prompt the need for different architectures and communication paradigms as we look ahead into the next-generation control systems.

Scope and Technical Approach

The objectives of this research will be achieved in several tasks:

- Task 1 research activities will be conducted at the University of Illinois, with support from PNNL. The initial research task will last 6 months and will include internal testing at the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) test bed housed at the University of Illinois and built as part of a large National Science Foundation (NSF) Cyber Trust Center focused on developing a trustworthy cyber infrastructure for power, ref: tcip.iti.uiuc.edu. The work in this task will leverage existing and ongoing work in the TCIP NSF Cyber Trust Center, which is addressing similar issues with a more basic research focus.

Other potential tasks include:

- Task 2 - development, testing, validation, and enhancements of the infrastructure designed in Task 1. In this task, the TCIP test bed would be used extensively for testing and validation. In addition deployment of the prototype at PNNL to test the developed technologies at the EIOC and associated SCADA research laboratory would be explored; e.g., to conduct laboratory vulnerability assessments of the operational security architecture. Problems discovered during validation would be corrected by the TCIP team and the enhanced system will be re-tested in an iterative manner.
- Task 3 integrates the results of Tasks 1 and 2 to develop a recommended architecture for secure, real-time and monitored communications for integrated wired and wireless networks

The security architecture developed in the proposed approach will address threats to the electric infrastructure and develop capabilities for an integrated, secure, timely and monitored communication infrastructure. The specification of the architecture needs to include both a documented design and a set of implemented software tools that instantiate the design. Furthermore, the design and implementation will influence each other in a continual process that results in the final security architecture.

The TCIP team shall design and develop techniques and algorithms for next-generation control systems that will be implemented in addressing communication between substation equipment and between substations and the control center. The software implementations shall be deployable in modern control systems with COTS operating-system-based devices and workstations.

The following considerations shall be included in the security architecture analysis: 1) key management for workstations, substation gateways as well as end-use devices, 2) real-time secure communication software that enables secure and timely communication between end-use devices in the substation over a Layer 2 Ethernet network, 3) real-time secure communication software that enables secure and timely communication between the gateway and the control center over a wide-area routed Internet Protocol network, 4) IDS that will run at gateways the control center to detect attacks against both the control system infrastructure and the enterprise business infrastructure, and 5) security state estimation system that runs at the control center to analyze alerts sent by the intrusion detection system via correlation and estimation.

Trustworthy Cyber Infrastructure for the Power Grid (TCIP)

Lead: Pacific Northwest National Laboratory, Jeff Dagle

Participants: University of Illinois at Urbana-Champaign, Cornell University, Dartmouth College, Washington State University, National Science Foundation

Purpose

The NSTB is supporting the TCIP initiative managed by the NSF. The TCIP NSF Cyber Trust Center was created in August 2005 to address the challenges of how to protect the nation's power grid. TCIP is working to provide the fundamental science and technology needed to create an intelligent, adaptive power grid that can survive malicious adversaries, provide continuous delivery of power, and support dynamically varying trust requirements.

Background

This task is intended to provide technical peer review oversight to the TCIP Initiative, and to better align the TCIP Initiative activities with DOE goals and objectives consistent with the Roadmap. The funding provided enables NSTB to attend a TCIP program review meeting to remain educated on current TCIP research. NSTB will then potentially be able to apply this knowledge to support the use of these new/emerging technologies by industry and asset owners.

Goals and Benefits

The TCIP Initiative, led by the University of Illinois at Urbana-Champaign and managed by the NSF, seeks to conduct long-term research that will provide the technology necessary to create a trustworthy cyber infrastructure for the power grid that provides reliable and secure information to system operators to better manage the power grid. This effort addresses several long-term R&D needs identified in the Roadmap. This task is intended to better align the TCIP Initiative activities with DOE goals and objectives consistent with the Roadmap.

Scope and Technical Approach

This work package will be executed by TCIP NSF Cyber Trust Center.

Wireless Sensor Networks and Applications to Electric Power Systems

Lead: Oak Ridge National Laboratory, Wayne Manges

Participants: ISA, Pacific Northwest National Laboratory, CenterPoint Energy, Argonne National Laboratory

Purpose

Much has been attempted in getting state-of-the-art security measures introduced in PCS and SCADA systems, especially in industries identified as "critical" to the nation's infrastructure. The asset owning community continues to resist the adoption of various security options available, primarily because no data has been available to support characterization of the likely impact on existing operations. ORNL

promotes a standards-based environment to provide an analytical basis for estimating the potential impact of options considered for security on critical performance parameters; for example, on throughput, latency, and reliability. The need for performance metrics is identified in the *Roadmap to Secure Control Systems in the Energy Sector* as a critical priority.

Background

ORNL will continue to support the ISA100 standards (Wireless Industrial Automation) development activity providing focus on the needs of the electric power industry. ORNL will support the new ISA100 sub-committee formed in 2007 focused on wireless "trustworthiness". Wayne Manges, as sub-committee co-chair (with Tom Mix from NERC) will provide leadership to the "Trustworthy Wireless Interest Group" through bi-monthly telephone meetings and at least four face-to-face meetings during the year.

Scope and Technical Approach

As part of this effort, Wayne will lead a group, comprising ORNL, DOE/OE, ANL, and PNNL staff, in working with Tom Flowers from a power producer company, in developing a paper for publication outlining concerns in the power community around the interactions among policy, regulatory compliance, and technological options regarding deploying wireless technology in critical-infrastructure-protection designated sites.

ORNL will continue to integrate this work with on going activities with DHS and DOE/EE related to wireless deployment in industrial sites.

INTEGRATED RISK ANALYSIS

Annual Risk Analysis Workshop

Lead: Sandia National Laboratories, L. Phillips

Purpose

The purpose of the "workshop" work package is to show the reduction of the overall risk of energy disruptions caused by control systems failures by applying the tools and capabilities that are being developed. A scenario will be developed with input from industry that addresses problems they are interested in. Each of the work packages will apply their tools and capabilities.

Background

Valuable tools, technologies, and processes have been created under the NSTB Program to assist in meeting the priorities identified in the *Roadmap to Secure Control Systems in the Energy Sector*. Industry and stakeholders should be aware of resources that exist today in the NSTB. A mechanism must be created to easily engage industry; matching needs with innovative technologies and methodologies. Feedback has been received from industry to indicate the need for greater awareness and understanding of how to inject their participation into the NSTB Program. Potential customers include industry owners/operators (oil, gas, electricity), vendors, policy makers, other government related programs. The objective of this task is to increase awareness and generate participation in the NSTB via a year-end workshop. This Annual Risk Analysis Workshop links stakeholders with risk-reduction tools, technologies, and processes needed developed under the NSTB program.

Scope and Technical Approach

The approach and scope for this task includes interaction with all Sandia related tasks for preparation and delivery of demonstrations and briefings at the workshop. Understanding the deliverables being produced under the NSTB Program is necessary in order to match stakeholder needs with available tools and technologies. Ongoing activity will culminate in a year-end workshop to be held June 2008. This workshop will provide a showcase of deliverables and facilitate one-on-one discussions with stakeholders. The targeted workshop audience will include asset owners, vendors, government, labs, and policy makers in the electricity sector.

Consequence Modeling

Lead: Sandia National Laboratories, Bryan Richardson and Randall Laviolette
Participants: TBD

Purpose

The Consequence Modeling work package will provide asset owners the "cost" associated with an electric power disruption. This work package will develop a software tool for estimating the consequences of a system failure to the serving utility on a local level. This will allow utility owners to quickly assess what physical assets are at the highest risk and explore mitigation options to reduce those risks. In addition, this work package will provide the requirements necessary to interface the impacts to existing regional and national level consequence models available at SNL. Consequence analysis allows direct comparison of otherwise incommensurate impact descriptions. This enables government policymakers to deal with the most consequential threats first, government funding agencies to allocate risk-reduction budgets more effectively, utility owner/operators to get the most out of their mitigation budgets, and cyber security

providers to prioritize their development efforts, all based on what will provide the greatest reduction in risk.

Background

Understanding the consequences of utility system failure is necessary to reduce critical infrastructure risk. To control risk, you need to measure it. Risk is a function of consequence, threat, and vulnerability, so to control risk, you need to understand consequence. Understanding consequences of cyber threats is vital to meeting many of the goals outlined in the *Roadmap to Secure Control Systems in the Energy Sector*, such as Developing and Integrating Protective Measures, Detecting Intrusion and Implementing Response Strategies, and Identifying Strategic Risks, to name a few. These solutions rely on knowing the consequence of a cyber threat so the appropriate response can be taken. This work package aims to increase our understanding of consequence.

In the area of critical infrastructure protection, consequences can be defined at local, regional, and national levels. Each level can contain consequences that affect other critical infrastructures. Methods for modeling the consequences of physical impacts of a cyber-attack on a control system for critical infrastructure protection are necessary for determining what threats and threat-vectors a control system requires protection against.

Physical system impacts don't affect all end-users in the same way. For example, losing power to several residences for several hours may have little impact on dollar cost, but losing the same amount of power over the same several hours at an industrial plant could lead to millions of dollars in lost production, which could then lead to adverse consequences in other critical infrastructures.

Goals and Benefits

Interface control documents (ICDs) between this work package's consequence analysis tool and physical impact simulators, such as the Virtual Control System Environment (VCSE) and the Impact Analysis of Cyber Attacks on Control Systems analysis tool (ICD) will be developed. Interface control definitions for existing Sandia consequence models will also be developed. The ICD will specify the requirements necessary for the integration of these risk analysis models.

This too is part of the Consequence segment of the Sandia Threat-to-Consequences risk perspective, linking physical system impact results and consequence analysis capabilities in the Threat-to-Consequence Model. The tool will take as input impact results generated from the *Impact Analysis of Cyber Attacks on Control Systems* work package and a class of threat vectors identified in the threat scenario of the Threat Characterization work package. The consequence analysis engine will then be used to quantify the consequences of the input threat vectors for a given utility. A software implementation of the consequence-ranking framework will be developed to assist in the creation of the value tree. The resulting software will then be used to analyze the results generated from the analysis engine against the value tree. The consequence analysis tool will provide a total consequence *performance index* for each threat vector class analyzed, as well as a value for each impact category that illustrates the negative effect (disutility) the treat vector imposes on the impact category.

Scope and Technical Approach

Subtask 1: Sandia will continue work on the Sandia/MIT consequence software framework from FY07. This work will focus on supporting simultaneous multiple failures within the framework, as well as refining the user interface to ease the burden of creating and modifying the value tree.

Subtask 2: Sandia will continue work on exploring existing Sandia consequence models to help determine what is required for assessing the consequences of an event at the local, regional, and national level. This

work will focus on the continuing development of data sets/formats and interface definitions for the existing consequence models (including the one being developed as part of this task – local perspective) as well as SNL proprietary's Critical Infrastructure Modeling and Simulation tools (regional and national perspective) such that they can seamlessly interoperate with the effects and impacts models being developed in the other tasks.

Impact Analysis of Cyber Attacks on Control Systems

Lead: Sandia National Laboratories, Jason Stamp and Richard Colbaugh
Participants: New Mexico Institute of Mining and Technology

Purpose

This task provides a means to estimate electric supply interruptions that can be caused by cyber attacks. Given a power grid and its associated control system, this task will help answer the question of what significant electric supply interruptions are plausible given a power grid model and certain vulnerabilities or attacks. The generated output will allow stakeholders to address those vulnerabilities whose exploitation would cause the biggest impact and enable an optimal risk reduction strategy. This task will deliver mathematically proven models that will predict cyber attack impacts on the physical power system infrastructure.

Background

The *Roadmap to Secure Control Systems in the Energy Sector* identifies a critical need to better understand the possible impacts of attacks on electric power systems in order to better prioritize mitigation investment to control risk. The roadmap also points out that "asset owners are hard-pressed to justify … control system security" because they are unable to "quantify and demonstrate the potential impacts of cyber attacks on energy sector control systems." This work package addresses lack of understanding of the impact of cyber attacks on the power system.

To control risk, you need to measure it. Risk is made up of consequence, threat, and vulnerability. The consequence of an event is its cost in terms of dollars, health, environmental problems, quality of life, loss of reputation, etc. To compute the consequences of an attack on the power system you need to know the attack's impact, that is, all of the effects of the attack on the power system itself. In short, to control risk you need to understand impact. This work package aims to increase our understanding of the impact of cyber attack.

Note the *existence* of the threat will be brought to our attention by the Plausible Threat Characterization work package products. The *effects* caused by an exploited vulnerability on the power systems control system infrastructure will be provided by the VCSE work package. The *consequences* of the infrastructure impact will be analyzed using Consequence Modeling work package products. If two attacks had similar impact on the power system, we would look at products to decide which had the greater consequence.

There are significant technical challenges: the existing infrastructure is large and complex, the problem is inherently uncertain (e.g., the behavior of both the attackers and the infrastructure is probabilistic), and we need quantitative, scientifically rigorous impact assessments. Previous approaches to analyzing the system-wide impact of attacks and perturbations to infrastructures have included: 1) ad hoc analysis (involving, for example, subject matter experts performing reductive analysis via hierarchical risk

decomposition), 2) static analysis (e.g., based on studies of system equilibria), and 3) basic "brute force" methods (e.g., requiring extensive and expensive computer simulations of outage permutations). These techniques are useful and do provide insight into infrastructure failure mechanisms but ultimately none provide a way to study threat impact.

Furthermore, we need an answer *quickly* and *inexpensively*. The approaches we use today—lab prototyping using simulators, field testing, and hybrid simulation environments such as the VCSE—provide results only with considerable modeling detail and significant time and resource investments. This work package will deliver tools that will provide "so what" answers quickly and cheaply to help utility owners, technology providers, and government policymakers and funding agencies better understand how concerned they should be over each newly discovered threat and vulnerability.

Goals and Benefits

With cyber attack impact knowledge in hand, government policymakers could deal with the most consequential threats first, government funding agencies could allocate budgets more effectively, utility owner/operators could get the most out of their mitigation budgets, and cyber security providers could prioritize their development efforts, all based on what would provide the greatest reduction in risk.

In the Sandia risk perspective (ranging from threats to consequences), this project specifically addresses impacts to electrical grids. This will enable other projects (such as Threat Characterization) to evaluate and rank the potential importance of cyber vulnerabilities and attacks in terms of risk by providing an estimate of the potential effects. Then, especially for similar impacts, further analysis based on quantified results (such as Consequence Modeling) may be undertaken. Current practice, which relies on expert opinion and consensus, does not quantify threats and vulnerabilities based on impact. The effects of hypothetical migration approaches can be modeled as attenuations to the effects of vulnerabilities in the power grid, and subsequently we can calculate "impact reduction" they provide to calculate a rough cost-benefit. Finally, interactive use of the proposed tool may allow more free-form investigations of grid impacts, so that patterns of effects that could lead to big consequences might yield insight into vulnerabilities or attack scenarios that we haven't considered yet.

To summarize, we need to better estimate attack impacts before resorting to simulations or expensive lab/field tests. This work package will deliver algorithms and an interactive tool that will provide a quick, cost-effective process to:

1. Identify plausible impact approaches, and
2. Assess the disruption to the power-grid, given a particular attack.

Customers include utility owners and operators, technology providers, national labs, and government policymakers and funding agencies.

Scope and Technical Approach

This effort is a continuation of the FY07 work package. In FY07, the following results were obtained:

- Defined the cyber-to-physical bridge by which a cyber attack translates into physical effects on the grid
- Attack scenarios: Plausible attack scenarios were defined given particular effects
- Realistic impacts: The power grid effects caused by a given attack scenario were observed in a power grid control system model.

In FY08, this work package will continue to develop the existing algorithms and models to facilitate investigation of three new areas for impact analysis, all related to adversary manipulation of the control set-points (or "settings") in the control systems for the electrical infrastructure:

- Characterize patterns of cyber attacks that can affect control systems settings and thereby significantly impact a power grid
- Determine whether a given, finite attack budget for an adversary will be sufficient to cause a significant impact
- Investigate whether a sensitivity analysis-based approach can be applied to the dynamic hybrid power grid / control system model to determine potential targets for an adversary intending to cause a blackout.

The FY08 activities include three subtasks:

Subtask 1: Develop second-generation versions of the dynamic finite-state algorithms (delivered in FY07) that will allow broad impact analysis and finite-state decomposition for larger and more complex systems, including additional control system elements as well as nonlinear circuit effects for magnetic devices in the electric grid.

Subtask 2: Develop a new analysis capability to evaluate the impacts of malevolently-altered settings for grid control elements; and

Subtask 3: Conduct an analysis of the sensitivity concept: Determine whether the finite-state abstracted model can give quantitative information on the minimum set of targets for a hypothetical adversary on either the physical grid or the control system necessary to have significant impact on the electrical system.

Plausible Threat Characterization

Lead: Sandia National Laboratories, J. Michalski

Participants: Georgia System Operations Corporation, OPUS Publishing Inc.

Purpose

The Plausible Threat Characterization work package will provide a framework and tool for leveraging open and closed source data to better quantify the level of threat in terms that are meaningful to the energy asset owners. The threat characterization framework and tool will enable asset owners to receive actionable, well-defined threat information that is unclassified. The deliverables from this work package includes: (1) a generic threat profile framework that provides a path for classified information to be declassified and used in an unclassified setting; and (2) a discovery tool that takes as input a set of cyber-vulnerabilities and attempts to discover and assess evidence that an adversary is interested in exploiting them. Information generated from this work package will reduce the risk of energy disruption by providing utility owners with prioritized, actionable threat information to facilitate corrective mitigation actions to be taken against the threat.

This work package is a continuation of work that was initiated in the late FY06 period of performance (POP). Deliverables include a Threat Analysis Framework document, which describes the elements necessary to provide a comprehensive approach to threat analysis, and a Generic Threat Profile document that will be used to identify threat characteristics necessary to assess the threat capability in unclassified terms.

Background

The Plausible Threat Characterization subtask will provide a framework and tool for leveraging open and closed source data to better quantify the level of threat in terms that are meaningful to the energy asset owners. The threat characterization framework and discovery tool will enable asset owners to receive actionable, well-defined threat information that is unclassified. The deliverables from this task include a discovery tool that takes as input a set of cyber-vulnerabilities and attempts to discover and assess evidence that an adversary is interested in exploiting them. Information generated from this task will reduce the risk of energy disruption by providing utility owners with actionable threat information to facilitate corrective mitigation actions to be taken against the threat.

Goals and Benefits

This work package fits in the Threat component of SNL's end-to-end, Threat-to-Consequences Model. The overall goal of this work package is to provide a means by which a utility owner can decide which threats matter the most. This will enable an effective and efficient protection response. The capability being developed under this work package will provide utility owners/operators (oil, gas, electric) with information concerning the abilities of adversaries and the likelihood that the adversary is capable and willing to attack energy sector resources. A greater understanding of the threat will enable utility owners and technology providers to better design, develop, and deploy appropriate defenses to defend against the more sophisticated threat.

Scope and Technical Approach

An additional issue to be considered when evaluating the risk associated with a given vulnerability or threat is the likelihood of an attacker identifying and exploiting the vulnerability. While many intelligence analysts recognize the importance of this question, there is at present little in the way of a systematic and comprehensive method for answering it.

The approach we are using to answer when evaluating the risk associated with a given vulnerability or threat is the likelihood of an attacker identifying and exploiting the vulnerability, is to computationally explore of large sets of potentially relevant data and identify unusual structures and behaviors in this data. A web crawler "seeded" with relevant keywords gathers and returns potentially relevant web pages from the world-wide web. Information in the web pages is extracted and stored for further data analysis, including graph analysis. In graph analysis we will develop a relationship diagram based on concept co-occurrence. This diagram forms a "concept-concept" graph that can be analyzed to discover new concepts that are not only relevant to our discovery task but are not already known keywords. This identification of previously unknown concepts that co-occur significantly with known keywords makes this process a *discovery* tool. SNL has had some success applying this graph-based analysis in different, but similar, domains. We anticipate similar results from this effort.

Virtual Control Systems Environment (VCSE)

Lead: Sandia National Laboratories, G. Conrad
Participants: DTE Energy, U.S. Air Force (Air Force Research Laboratories)

Purpose

Given a plausible threat, the Virtual Control System Environment (VCSE) work package will help asset owners and analysts understand what effects can be achieved on control systems if the threat were to be realized. This work package will develop a modeling and simulation tool that can be used to analyze and assess threats and cyber vulnerabilities on control systems (CS) without risking disruptions to critical

operations. The tool will also provide the means for evaluating selected mitigation options. The VCSE will permit the end-user to configure a simulation environment of control system devices and network communication protocols and enable real-time, hardware-in-the-loop connectivity for the purpose of understanding the effects of cyber-vulnerabilities on CS. The VCSE will reduce the risk of energy disruption by providing a realistic setting designed to replicate portions of a vulnerable infrastructure against which cyber attacks can be played out and effective mitigation tactics developed with no threat to the actual infrastructure.

Background

The *Roadmap to Secure Control Systems in the Energy Sector* established as Goal 1 to "Measure and Assess Security Posture". The VCSE tool will enable collaborative analysis for the determination of the robustness of a system's security posture by performing analysis on the modeled SCADA or control system. Goal 2 of the Roadmap (Develop and Integrate Protective Measures) defined the following as a key challenge: *Security upgrades are hard to retrofit to legacy systems, may be costly, and may degrade system performance.* The VCSE tool will support the design, integration, and evaluation of security solutions used in legacy systems.

Modeling tools such as the VCSE are needed to combat the challenging technological complexities associated with securing not only legacy systems but also for the integration of emerging control system components and system architectures. As control system architectures grow in complexity and interconnectivity with other networks, exposure to more sophisticated threats, and the trend toward incorporating conventional IT solutions, modeling and simulation tools will be needed to assist asset owners in making better-informed decisions in the selection of security solutions for their current and next-generation systems.

Goals and Benefits

The VCSE simulation environment will provide the following functionality (categorized in four capability areas): simulation framework; simulation configuration; simulation execution; and analysis tools.

I. Simulation Framework – This capability is the software that is associated with the core/kernel elements of the VCSE architecture. This consists of the following elements:

- Simulation Engine {scheduler, configuration, execution} – this feature is the "heart" of the tool and provides the environment for running simulations;
- Interoperability-federation Interface – this mechanism enables 3rd party simulators/ models to interact with VCSE (power simulators, both static and dynamic, custom models provided by asset owners, etc.); and
- External Integration {emulated devices, simulated device, and real hardware devices} – this feature provides the fusion of various levels of modeling fidelity.

II. Simulation Configuration – This capability allows the analyst access to the VCSE tool-box for building the targeted Control System (CS) environment under investigation. This includes identification of data inputs/outputs; CS simulated or emulated devices and communication protocol models. This capability consists of the following elements:

- A User Interface (UI) – allows the configuration and management of the simulation environment (i.e. devices, models, probes, data input/output, etc.);
- CS simulated/emulated devices – provides a suite of simulated and emulated CS equipment/components; and
- Network protocol simulators – provides a suite of network protocol models (ModBus, TCP/IP, DNP3, ICMP, ICCP, etc.).

III. Simulation Execution – This capability provides the ability to run and manage the simulation runs and includes statistics collection of data measurements for post-run analysis. The output generated from this capability will be used by several end-users, including: CS operators/ engineers, security operators/engineers; network analysts/designers; and CS product designer/engineers. This capability consists of the following elements:

- Setting data probes in the simulation environment for gathering post-analysis data;
- Managing the simulation runs (set static parameters, pause, resume, change run-time parameters, direct running output to visualization tools, etc); and
- Simulation environment library (store and recall a simulation environment for future use).

IV Analysis Tools – This capability is an extension of the VCSE tool-box and will allow the end-users the ability to perform post-simulation analysis. It will provide a mechanism for viewing the results of the simulation. It is envisioned that several visualization tools will be available to the user (i.e., 2-D/3-D views, data tables, graphs, charts, etc). This capability consists of the following elements:

- Graphical User Interface (GUI) for post-simulation data graphics display capability (2-D, 3-D, etc); and
- Data reduction analysis library.

Scope and Technical Approach

Given a cyber-threat, the Virtual Control System Environment (VCSE) task will help asset owners and analysts understand what effects can be achieved on control systems if the threat were to be realized. This task will develop a modeling and simulation tool that can be used to analyze and assess threats and cyber vulnerabilities on control systems (CS) without risking disruptions to critical operations. The tool will also provide the means for evaluating selected mitigation options. The VCSE will permit the end-user to configure a simulation environment of control system devices and network communication protocols and enable real-time, hardware-in-the-loop connectivity for the purpose of understanding the effects of cyber-vulnerabilities on CS. The VCSE will reduce the risk of energy disruption by providing a realistic setting designed to replicate portions of a vulnerable infrastructure against which cyber attacks can be played out and effective mitigation tactics developed with no threat to the actual infrastructure.

Subtask 1: Framework and Visualization System Improvement

This subtask will comprise the continued improvement of the core VCSE framework capabilities to achieve technology readiness level 7 by the end of FY08. This task incorporates the improvements and testing of the new capabilities as they impact the framework. Specific augmentations to the device library will include a generic HMI, actuator, IED, and a PLC. Work will also begin on incorporating the ICMP protocol into VCSE. Improvements will be made in:

- Device Management – Build a taxonomy and search capabilities for the various virtual devices allowing analysts to choose from an ever growing set of entries.
- GUIs – Many of the existing simulation configuration capabilities are tabular. These interfaces will be upgraded to a common look and feel and use greater GUI capabilities.
- Simulation management – Currently these tasks are done in C++ code for each simulation. These interfaces will be updated to allow the simulation components to be managed and save via GUI components
- Data collection – Build GUI components that allow the configuration of data collection for each simulation configuration.

- Analysis – As analysis experiments are performed analysis tools will be incorporated into the VCSE suite of tools. VCSE will be adjusted as needed to ensure that data is collected in applicable formats to the analysis tools.

Subtask 2: Federated Interfaces
This subtask will provide the VCSE mechanisms that will enable it to communicate with existing (commercial or otherwise) modeling and simulation tools. Communication protocols such as HLA need to be incorporated into VCSE to allow federation with capabilities such as RTDS (Real Time Data System) and MatLab.

Subtask 3: Simulation Development and Validation
This subtask involves the exercising of the overall VCSE capability to perform experiments of interest to both government and industry. Activities will include industry outreach to determine scenarios of interest and the developments of those scenarios within VCSE to provide partners with answers to their questions. This task will also support the Control Systems Risk Analysis Workshop that will be held at the end of the project. Specific interest will be made to address a simulation of ISO/RTO scale.

Subtask 4: VCSE Project Management
This task provides project management oversight for the overall operations of the VCSE work package. Activities associated with this task are: day-to-day management of the technical activities; the creation of a project plan and schedule for the development effort; establish software build-dates; provide cost, schedule, and performance status; manage internal and external interfaces; track changes, issues, and risks; and be responsible for the execution of the VCSE WP.

SYSTEM VULNERABILITY ASSESSMENTS

Assess Control Systems in Test Bed Facilities

Lead: Idaho National Laboratory, Dave Kuipers

Participants: Siemens TG, Telvent, OSI, Teltone Gauntlet, Argonne National Laboratory, ABB, ABB Consortium (Austin Energy, DTE Energy, Indianapolis Power & Light Company, ITC Transmission, Kansas City Power & Light (KCP&L), LCRA, the New York Independent System Operator (NYISO), Snowy Hydro Ltd., Tri-State G&T Association)

Background

SCADA, EMS, and DCS are used in the energy sector to control electricity flow in transmission and distribution lines, and oil and gas flow in pipelines. These control systems automate many of the functions and processes of energy infrastructure systems and are essential for efficient and reliable operation. Significant increases in the use of digital control systems and interconnected communication and data networks have led to major improvements in operational efficiency and reliability. However, during the design and installation of these digital systems little consideration was given to the possibility that someone with malicious intent might use electronic/digital (cyber) methods to attack the system and disrupt operation. As a result, significant vulnerabilities exist that in many cases are susceptible to exploit. There have been very few reported incidents of cyber attacks on critical control systems, and therefore, it is difficult for industry to justify expending resources to improve (harden) their systems against such an attack. Given the national importance of maintaining critical infrastructure, government support for improvement efforts is needed.

The *National Strategy to Secure Cyberspace* recognizes that critical infrastructure control systems are vulnerable to cyber attack and calls for the public and private sectors to work together to ensure those systems are protected. The *Strategy* directs DHS and DOE to work in partnership with other agencies and the private sector to develop best practices and new control system security technologies. Homeland Security Presidential Directive 7 (HSPD-7) designated DOE as the Sector-Specific Agency to lead the federal government's efforts to help protect critical energy infrastructures from physical and cyber attacks.

In 2005, DOE/OE facilitated a joint industry-government effort to prepare an integrated plan to define and guide the actions needed to achieve a significant security improvement in the energy sector. The outcome of that effort was the report, *Roadmap to Secure Control Systems in the Energy Sector*. The Roadmap identifies needs across a broad range of technology, business, and awareness issues. The NSTB Project supports many of the actions included in that plan.

INL activities performed under this project have been primarily devoted to identifying vulnerabilities in energy sector control systems. Working with control system vendors and owners, project staff have performed cyber vulnerability assessments and reported the results, including recommended mitigations, back to the industry partners. The partners have responded with improvements to their systems/products and those improvements are being deployed in the energy infrastructure.

Cyber vulnerabilities and mitigations are identified through two separate but closely related assessment activities. The first is performing control system cyber assessments in the SCADA Test Bed; the second is performing assessments at operating utility systems. The systems undergoing assessment in the test bed are obtained from SCADA/EMS vendors and are representative of the new systems entering the market. The vendors who participate in this project currently provide more that 85% of the SCADA systems to the energy sector; therefore, significant improvements in these systems can have broad impact on the energy infrastructure.

Scope and Technical Approach

The control systems are selected for assessment based on their prevalence in the energy infrastructure and on the willingness of industry partners to participate in the assessments.

The following sequence is typically followed:

- A major vendor in energy sector control systems provides the control system, provides limited training, and provides technical support in setting up the system in the test bed. At the time the first collaboration with a given vendor is initiated, a CRADA is negotiated to establish scope, roles and responsibilities to ensure protection of sensitive information.
- An assessment plan is developed to identify specific functions of the system to be examined in the assessment.
- The system is operated within the test bed environment and a team of cyber researchers attempts to disrupt its operation through cyber attacks
- Vulnerabilities that are found during the assessment are documented in a proprietary report to the vendor. The report includes recommendations for mitigation approaches the vendor might use to reduce vulnerabilities.

SCADA systems to be assessed within this subtask include the following:

- Siemens (Phase 2, planning completed in FY-07)
- Telvent (Phase 2, planning completed in FY-07)
- OSI (Phase 2, planning completed in FY-07)
- ABB Consortium NMR3 (follow-on to Phase 2)

Cyber Vulnerabilities in Industry Technologies

Lead: Idaho National Laboratory, Dave Kuipers
Participants: TBD

Background

This subtask is a follow-on research task to the electrical substation assessment work to further evaluate existing and emerging industry technologies associated with control systems. These technologies provide intelligent controls, expanded communications capabilities and utility functionality that have yet to be evaluated by the NSTB program but are intrinsic to operation and support of the electrical grid systems. This study will evaluate what compromises to these technologies may affect control systems and what impacts they would have on grid operation. The primary objective of this task is to determine a path forward in assessment of technologies not currently being performed by the NSTB.

Scope and Technical Approach

Asset owner and vendor experts along with available information will be utilized in a study to evaluate technologies not currently being addressed but may prove to be important in their impact to grid control systems cyber security. Some of the potential areas of interest include potential cyber vulnerabilities in control center and substation equipment, communications protocols and media, and interfaces with other systems and processes such as Advanced Metering Infrastructure and demand response, automatic generation control, substation automation, and potentially distributed generation.

Identification of Cyber Vulnerabilities in Electrical Substations

Lead: Idaho National Laboratory, Dave Kuipers

Participants: Newton-Evans, Oncor Electric Delivery, PacifiCorp, others TBD

Background

NSTB cyber vulnerability assessments to date have focused on control systems located in control centers and on specific devices and protocols used in protecting data essential to the reliable and efficient operation of the electric grid. Compromises to these control systems could have major impacts on grid operation. However, the most significant grid impacts occur when the control systems are used to manipulate systems and equipment in the field, much of which is located in substations. One objective of this task is to determine the extent to which substations are vulnerable to directed cyber attacks and to provide recommendations for mitigation of common vulnerabilities identified. This is a direct response to the Roadmap priority of identifying best practices for physical and cyber security for remote facilities.

Scope and Technical Approach

The task will be performed in two phases. The first phase will include a study of current and emerging technologies, standards and configurations associated with substation automation and a high level analysis of communications and cyber vulnerabilities associated with the technologies and applications. The study will develop a methodology and framework that prioritizes potential vulnerabilities by risk. The framework will be used to prioritize future work. The study will be documented in a report written at an unclassified level. Industry advisors will be consulted to support and validate the findings of the report.

In the second phase of the task an asset owner will be selected that is interested in working together to identify typical cyber vulnerabilities in electric substations that, if exploited, could result in significant disruption to grid operation. Specific functions and the communication paths and technologies used in performing those functions will be examined to determine whether they appear to present a potential attack path into the substation.

Based on the information gained in the evaluation and assessment made by the team and the asset owner, generic lessons learned will be shared with industry for use in improving security. Some of the potential areas of interest include cyber attacks on substation equipment (breakers, switches, transformers, instrumentation), and several communication protocols and media (including wireless communications).

This is a first of its kind assessment and costs and schedules are based on experience in working with vendors and asset owners in the execution of on-site assessments of SCADA/EMS installations. The project subtask will be initially setup and industry partners will be identified. The CRADA process is assumed to be comparable to that experienced in the establishment of CRADAs with other industry partners. Assessment planning will be performed in parallel with CRADA approval and the assessments will start 8 months after task initiation. The assessments will follow the processes and schedules established for on-site assessment of utility control centers and each will require planning, pre-assessment visit, evaluation and final planning, on-site assessment, analysis and reporting, and closeout. The on-site assessments will be performed by 4-member teams.

On-Site Vulnerability Assessment

Lead: Argonne National Laboratory, Shabbir Shamsuddin; Idaho National Laboratory, Dave Kuipers

Participants: Interstate Natural Gas Association of America (INGAA), American Petroleum Institute (API), American Gas Association (AGA), Oil/Natural Gas Asset Owner

Purpose

On-site assessments provide an opportunity to determine if the vulnerabilities identified in a laboratory setting are relevant in actual installations. The site assessments provide direct feedback to a specific asset owner on potential vulnerabilities and mitigations, present opportunities to identify good security practices, and support a "trial run" of the assessment tools that are being developed by INL under the NSTB program.

Background

An important objective with regard to achieving a secure control system is to identify existing and potential vulnerabilities and to then institute mitigation efforts that will neutralize, or at least minimize, these vulnerabilities. However, energy sector companies have limited ability to measure and assess their cyber security posture. There are no consistent metrics or risk assessment methodologies that enable companies to measure security risks and vulnerabilities.

Extensive cyber vulnerability assessments are being performed in a laboratory to identify potential vulnerabilities in the various systems being placed on the market by leading SCADA/EMS vendors. However, while significant effort is taken to establish a representative test environment (including appropriate communication paths, components, and network architectures), examinations of system configurations and system responses in an actual installation are needed to confirm validity and relevance of laboratory results.

Asset owners selected for on-site assessments are identified through a number of criteria including: installation of a system essentially the same as one examined in the laboratory test bed; the existence of an available development or other non-production system highly representative of the actual installed system; and a willingness to share with industry peers appropriate lessons learned and best practices identified during the on-site assessment.

An essential part of the on-site assessment is the application of assessment tools developed in the laboratory and in other on-site assessments, all leading to the ultimate objective of developing safe and effective tools that can be used by asset owners for conducting self assessments. Such tools support a priority in Goal 1 (Measure and Assess Security Posture) of the *Roadmap to Secure Control Systems in the Energy Sector*, "Fund efforts to develop tool set for owners and operators to conduct self assessments." This task also supports a priority in Goal 2 (Develop and Integrate Protective Measures) "Identify best practices for physical and cyber security of substations and control centers." The on-site assessments also address a challenge in Goal 4 (Sustain Security Improvements) "Limited knowledge, understanding, and appreciation of control systems security inhibit action."
On-site assessments by knowledgeable entities can provide this service to the stakeholders. INL currently offers such a service, primarily to asset owners in the electric industry. For the oil/natural gas sectors, member companies under INGAA and API have expressed an interest in participating in such assessments, with an objective of developing a self-assessment capability within its membership.

ANL will assist INL with on-site assessments of two to-be-determined operators in the oil and natural gas industries, working through the American Gas Association (AGA), American Petroleum Institute (API), and Interstate Natural Gas Association of America (INGAA) to support INL assessment efforts, both in its test bed assessment of Telvent products and in its on-site evaluation of oil and natural gas sector industry installations using those products. In-house industry expertise will enable ANL to relate test bed findings to actual operating situations. It will also enable ANL to support and guide security improvements within the operators' own systems.

This effort can be expanded to address a concern of the INGAA membership, the area of self-conducted assessments. INGAA would like to work with ANL and the multi-laboratory team to develop self-assessment expertise in-house. Existing self-assessment tools and/or methodology would be adapted to use within the natural gas transmission industry to accomplish this objective. This task can also support the goals and objectives of INL, SNL and PNNL for the oil and natural gas infrastructure assessments.

Goals and Benefits

The on-site assessment provides three significant benefits supporting improved cyber security in the oil and natural gas sector. The first is the identification of specific vulnerabilities in the asset owner's system (potentially none may be identified, in which the lessons learned would be extremely valuable as industry best practices—this has not yet occurred). Second is the communication of lessons learned by the asset owner to peers. This is a highly credible method of delivering security awareness as well as information on best practices to industry. The third benefit is continuing development and evolution of tools that can be used by industry for cyber vulnerability self-assessments.

Scope and Technical Approach

This ANL/INL effort will include scheduling, meeting and coordination with INL and industry partners in the oil and natural gas sectors to conduct on-site SCADA and control systems security assessments. In particular, it will include verifying that the recommended mitigations identified in the NSTB laboratory setting are relevant in actual installations. At present there is no formal effort to verify the NSTB findings in a true operational environment.

Subtask 1 -- Scope: ANL will assist INL in making contact, selection, and initial negotiation of a formal agreement with at least one company from oil and one company from natural gas sector to cover contractual requirements and a vulnerability assessment plan to document scope of work. This document has typically taken the form of a CRADA, which provides statutory protection over the information developed. Rules of Engagement (RoE) will be provided at an early stage to ensure a mutual agreement on the assessment activities and responsibilities.

Subtask 2 – Planning: ANL will assist INL in the Planning for the assessment that will be initiated with a pre-assessment visit and program review. These activities are designed to gain a thorough understanding of the oil and natural gas company, equipment, assessment boundaries, and share expectations. A basis to complete a vulnerability assessment plan will be developed, identifying the ToEs and RoE. ToEs will be based on a review of the selected company system, perceived vulnerabilities, and experience from previous assessments of the system in use by the company.

Subtask 3 – Assessment: After the approval of the vulnerability assessment plan, the assessment will be carried out. ANL/INL will perform an evaluation of the selected company's Internet presence and network topology. The onsite assessment will be carried out based on the vulnerability assessment plan; however, the experience and expertise of the INL cyber team and ANL team will be used to guide detailed analysis and the development of tools that can be applied to the onsite assessment and control system cyber vulnerability assessments in general. ANL will help guide the assessment to ensure critical

system functions are evaluated. At the conclusion of the onsite assessment a review of notable findings will be shared with the selected company.

Subtask 4 – Reporting: ANL will assist INL in the draft write up of a detailed report that will be prepared covering the assessment process, results, and recommended approaches to mitigating any vulnerability found. Internal records will be maintained to support repetition of the assessment. Review of the detailed report will be performed by the selected company representatives to ensure clarity and correctness. An out-briefing of the results will be held with the company, where a discussion of findings and a path forward for external sharing of lessons learned with asset owners to increase awareness in the industry.

PARTNERSHIP & OUTREACH

Industry Conference Participation

Lead: Idaho National Laboratory, Dave Kuipers

Participants: Siemens User Group (UG), ABB UG; OSI UG, Telvent UG, AREVA UG, General Electric (GE) UG, Energy Security Northwest CIP (E-SEC-NW CIP), Process Control Systems Forum (PCSF), NERC CIPC, PJM Operations, CIGRE WG D2.24 (International Council on Large Electric Systems), ANL, AGA, Association of Oil Pipelines (AOPL), API; INGAA, Multi-State Information Sharing and Analysis Center (MS-ISAC), National Association of Regulatory Utility Commissions (NARUC), National Petroleum Refiners Association (NPRA), SmartGrid, Platts, Society of Workforce Planning Professionals (SWPP), Solid State Energy Conversion Alliance (SECA), SANS Institute, others TBD

Background

Results from the cyber vulnerability assessments have been communicated to industry in two general types of conferences. The most detailed presentations have been made in the user group meetings held by the individual SCADA system vendors. The audience in these meetings is somewhat restricted through their business relationship with the vendor and details specific to the assessment results of that vendor's SCADA system can be shared without a significant concern about releasing business sensitive information. To reach broader audiences in more open security related conferences, the level of detail is reduced and vulnerabilities and methods of mitigation that are common to more than a single vendor are discussed. In both of these forums, the objective is to enhance audience awareness and understanding of control system vulnerabilities and of the mitigation options that are available to them.

Scope and Technical Approach

Presentations at general conferences are typically in response to invitations from the organizers to share information gained in the NSTB program. In some cases, NSTB participation as a panelist is requested. In the user group meetings, presentations typically involve a joint presentation with a representative from the applicable vendor to support a more comprehensive description of the vulnerabilities, recommended mitigation, and the action the vendor has taken or will take to address the issues. These meeting also present an opportunity to provide SCADA system owners with information they can use in taking their own action to address vulnerabilities in the system of interest.

NERC CSSWG Support

Lead: Pacific Northwest National Laboratory, Jeff Dagle

Participants: North American Electricity Reliability Corporation (NERC)

Background

The fundamental NSTB product is new knowledge gained through assessments, analysis, and R&D. Effectively sharing that knowledge with industry stakeholders who can use it to enhance security is essential to enhancing control system security in the energy sector. That sharing is accomplished through the Industry Outreach effort in a number of ways, including security training, reports, and presentations provided to industry. In this case it is achieved through PNNL's participation in NERC working group meetings on behalf of the NSTB Program.

An additional important outreach objective is to obtain information from industry related to needs that can be addressed through the NSTB Program.

Technical Approach

The NSTB has seen significant improvements in stakeholder awareness through participation in the NERC Control Systems Security Working Group (NERC CSSWG) of the Critical Infrastructure Protection Committee (CIPC), including the development of recommended mitigation strategies for NERC's annual "Top 10 Vulnerabilities" list. Funding for this task will allow PNNL to continue supporting and coordinating activities with the NERC CSSWG/CIPC on behalf of NSTB.

SCADA Security Workshops

Lead: Idaho National Laboratory, Dave Kuipers

Participants: Siemens UG, PCSF, SECA, SANS Institute, Red/Blue Team Partners, others TBD

Background

The NSTB SCADA Security Workshops provide several levels of control systems cyber security training to a variety of organizational disciplines. To date the program has provided this training to over 1800 people. The training program has proven invaluable in increasing the awareness of management and operations personnel in vendor and user organizations to the issues associated with control system cyber vulnerabilities and related topics. User organizations have initiated incorporation of cyber security concepts in their system upgrade project as a result of material presented in the workshops.

The INL has also developed and presented Red/Blue team control system cyber security workshop over the past two years. Funding from multiple sources has supported this work. The workshop trainer personnel are highly experienced cyber researchers and have presented several courses. The equipment utilized for the course is available and fully integrated to provide classroom and hands-on training that simulates an attacker group attempting to gain access to a business and control systems operation and a defender group attempting to detect intrusion and defend their operation.

Scope and Technical Approach

The workshop training is provided in User Group meetings, conferences and other gatherings where vendor and/or user management, technical and operations personnel are available to attend in groups sized to optimize the course. Depending on the schedule, multiple courses are often provided to diverse disciplines at a given meeting to maximize the exposure of the training to the target audience. The training material is updated periodically to provide current training information. Training presentation costs are shared with the customer. The NSTB program typically funds the trainers' labor costs and the demonstration system development support. The customer funds classroom-related expenses and the trainers' travel expenses.

The Red/Blue team training is provided at the INL. Several days of classroom training culminates in a full day red/blue team exercise monitored and scored by an INL white team, followed by a wrap up day of exercise debrief, evaluation and final training. This course has received excellent reviews and is very relevant to potential attack on control systems. This subtask would target utility control system cyber security-related personnel. The outreach aspect of this subtask is providing training and experience to utility personnel on actual cyber security incidents and the real-time aspects of a concerted attack. The attendees will fund their own travel and lodging expenses. The project will fund the trainers, system and

training preparation work, and facility fees for the training location. The training will be limited to domestic energy-sector personnel only. Attendee list and affiliation will be provided to DOE/OE prior to training course attendance.

APPENDIX A:
INDUSTRY PARTNERS

Industry Partner Project

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector